VERSION WITH MARKINGS TO SHOW CHANGES MADE

IN THE SPECIFICATION:

Page 1, the last paragraph bridging pages 1 and 2, was amended as follows:

--With such a method, electronic postage stamps can be obtained and printed on postal articles. The device, for example a computer, with which the electronic postage stamp is printed is thereto provided with a Postal Security Device (PSD), to which a unique identification code is related. The electronic postage stamp comprises various elements, of which a few are mentioned as "security critical": the identification code of the PSD, the value of the contents of an incremental register, the franking value of the postal article and a digital signature. The contents of the incremental register represent the total monetary value of all hitherto printed electronic postage stamps with the related PSD. The combination of identification code and the contents of the incremental register represents a unique bit string per postal article. Since the manner in which said unique bit string is composed must comply with a known rule, the value of a following unique bit string for a following electronic postage stamp can be predicted, which is disadvantageous in regard to possible [fraude] fraud.-

Page 3, the fourth full paragraph was amended as follows:

--According to the invention, each unique bit string used is thus centrally generated and registered, and said bit string is moreover coupled to the user who has bought an electronic postage stamp and/or the machine which prints the electronic postage stamps. It can thus not only be centrally detected whether the electronic postage stamps are used only once, but [fraude] <u>fraud</u> can also be easily traced to the source. Further, the use of a PSD can thereby possibly be waived.—

Page 3, the last paragraph bridging pages 3 and 4, was amended as follows:

--In a first embodiment, the unique bit string and the identification code, protected with the aid of a first message authentication code and/or protected by encoding, are stored, prior to step c, by a terminal on an information carrier with memory, step c taking place after the information carrier has been read in by a printing device. Such an information carrier can, for example, be a chip card, on which several such unique bit strings, together with the identification code, can be stored. The identification code can, for example, be derived from the number of the bank or

ATM (Automated [Counter] Teller Machine) card with the aid of his personal identification number (PIN).--

Page 6, lines 34 and 35 were canceled as follows:

[Advantageous embodiments of such a system are apparent from the sub-conclusions 11 up to and including to 20.]

Page 7, the first full paragraph was amended as follows:

--The present invention is also related to an exchange provided with a first central memory having a set of unique bit strings, a second central memory for storing the combinations of identification codes and provided unique bit strings, said combinations corresponding with franking marks which have been printed on a document, central input means for inputting franking marks printed on documents, a third central memory for storing combinations of identification codes and unique bit strings present on the inputted franking marks, and processor means connected to the central input means and the first, second, third central memories for mutually comparing the data in the second and third central memories. An "exchange" as used in the present application refers to a central station that has the first, second and third central memories.-

Page 9, the paragraph beginning at line 8, was amended as follows:

--In Fig. 1, reference number 2 refers to a terminal, which, for example, is set up in the wall of a post office. Said terminal 2 can communicate with a central station or an exchange 34, for example via the public switched telephone network (PSTN) 46. Communication paths via other networks are of course possible. In this case, use can be made of the Internet. Communication can also take place in other ways, for example via CDROMs, floppy disks, etc.-

Page 11, the fifth paragraph was amended as follows:

--Said information 29 comprises, for example, human-readable data 24 related to the mail-sending [organisation] organization (or other advertising), as well as a marking sign 26 (for example a bar code) enabling automatic orientation of the postal article in a stamping/sorting machine, and a franking mark 28, for example in the form of a two-dimensional bar code 28, which contains further, possibly encoded, information. Said franking mark 28 shall at least contain a unique bit string, of which the use will be explained further on, and an identification code. The identification code identifies the user, i.e. the person who purchased the electronic postage stamp, and/or the device with which the franking mark is printed. If the identification code is

coupled to the printing device, this can, for example, be a unique code associated with said SAM 19. In that case, the owner of the franking machine is responsible for possible [fraude] fraud with the use of electronic postage stamps.-

Page 15, the second full paragraph was amended as follows:

--For further protection of the whole, the processor 4 preferably sends a copy of the identification code with the issued franking numbers, protected by MAC1 and/or protected by encoding, to the exchange 34, which stores this information in memory 40 so that at a later stage possible [fraude] fraud can be checked centrally, step 218. This will be further discussed later.-

Page 17, the third full paragraph was amended as follows:

--Upon dispatch of the postal article 22 from a sender to a receiver, said postal article 22 will, at a given time, arrive in a sorting [centre] center. There said postal article 22 will be read in with the aid of the means 32, and it can be checked again whether said postal article 22 has been sufficiently franked. The means 32 read at least the franking mark 28. The means 32 thus collect all read-in franking marks 28 of all postal articles which are provided

therewith. All franking marks 28 are subsequently sent to the exchange 34 and are there read in by the processor 36 via the input means 44. Said processor 36 stores the inputted franking marks in the memory 42.—

Page 22, the last paragraph bridging pages 22 and 23, was amended as follows:

--A further option is to implement the system shown in Fig. 1 in such a manner that each of the franking cards 18 is also allocated a unique number. Possible [fraude] fraud with franking cards 18 can then be pin-pointed. Information related to said fraudulently used franking cards 18 can then be included on an arbitrary franking card 18. Subsequently, said information, related to the fraudulently used franking cards 18, can then be transferred "unperceived" to the franking machines 20, which store the related information in a memory (not shown). If a customer with fraudulently used franking card 18 wishes to print an electronic postage stamp, the franking machine 20 can detect the related franking card 18 and render it invalid. This can be done either by deleting the contents of the franking card 18 or making them non-readable, or by simply refusing to print an electronic postage stamp. Thereby further damages by possible [fraude] fraud can be decreased.—

Page 24, the third full paragraph was amended as follows:

--Fig. 4a shows [een] a flowchart of an embodiment of the functioning of the PC 50 in the context of the present invention for reloading a bank card 18 with a certain desired amount to be spent on electronic stamps. Fig. 4b relates to the actual printing of such an electronic stamp with such a bank card 18.--

Page 27, the last paragraph bridging pages 27 and 28, was amended as follows:

--It is also imaginable, however, to let payment be made later, as explained above with reference to the embodiment of Fig. 1. In that regard, the balance loaded in the bank card 18 does not represent a total amount which can be expended on electronic stamps, but the number of times that the franking number provided can be used. The advantage of post-payment is that the user does not need to weigh his postal article 22 in advance in order to have the correct franking value included in the franking mark 28. After all, the franking mark here too uniquely identifies the user, who can subsequently have the invoice sent to him or whose bank balance can be automatically debited. Moreover, the presence of the unique franking number with identification code and the actual "balance" guarantees that each postal article 22 is

uniquely identified, so that [fraude] fraud can be detected immediately.—

Page 28, the first full paragraph was amended as follows:

--It is further remarked that, instead of or together with an identification of the user, it is possible to include an identification of the SAM 64 in the franking mark. In that case, the owner of the PC 50 with SAM 64 is responsible for the correct payment of the electronic postage stamps and for possible [fraude] fraud carried out with the PC 50. It is then up to said owner to subject access to the program for purchasing an electronic postage stamp to [authorisation] authorization rules.—

Page 28, the second full paragraph was amended as follows:

--In a further embodiment with the aid of a PC 50, a standard PC without SAM 64 can be used. In this case, said PC 50 cannot safely calculate MAC's. The franking mark is then produced either centrally in the exchange 34 or in server system 70, and sent to said PC 50. Said PC 50 then combines the received franking mark with possible other information and prints this on the postal article 22 with the aid of printer 62. In that case, instead of working with the storage of a

balance for electronic stamps on bank card 18, one franking mark per time is retrieved from the exchange 34. In this case, payments of electronic postage stamps preferably take place directly either by debiting a user's bank balance, or from bank card 18 with an electronic purse. To contend with possible [fraude] fraud, the user must uniquely identify himself, for example with his giro/bank number and an associated PIN. Preferably, identification then still takes place with bank card 18 and by checking a PIN code.--

IN THE CLAIMS:

The claims were amended as follows:

--2. (amended) [A] The method according to Claim 1, [characterised in that,] wherein prior to step c, the unique bit string and the identification code, protected with the aid of a first message authentication code [and/]or protected by encoding, are stored by a terminal [(2)] on an information carrier [(18)] with memory, and step c takes place after the reading of the information carrier by a printing device [(20)].--

--3. (amended) [A] The method according to Claim 2, [characterised in that,] wherein besides the unique bit string and the identification code, a terminal identification code, protected with the aid of the first message authentication

code [and/]or by the encoding, is also stored on the information carrier [(18)] with memory by the terminal [(2)].-

--4. (twice amended) [A] The method according to Claim 2, [characterised in that] wherein after the reading of the information carrier [(18)] by the printing device [(20)], use of the unique bit string for printing a further franking mark on a further document is rendered impossible by the printing device [(20)].--

--5. (twice amended) [A] The method according to Claim 2, [characterised in that,] wherein after reading the information carrier [(18)], it is checked whether the value of a counter on the information carrier [(18)] lies within predefined limits, and, if this is the case, the value of the counter is adjusted after reading and step c is executed, and, if this is not the case, step c is blocked.--

--6. (amended) [A] The method according to Claim 1, [characterised in that,] wherein upon execution of step c, use is made of a computer [(50)] and a printing device connected thereto [(62)].-

--7. (twice amended) [A] The method according to Claim 1, [characterised in that] wherein the identification

code comprises a user identification code [and/]or a printer identification code.--

--8. (twice amended) [A] The method according to Claim 1, [characterised in that] wherein on the basis of the franking mark a second message authentication code is calculated and that this also is printed [and/]or the franking mark is printed in encoded form.--

--9. (twice amended) [A] The method according to Claim 1, [characterised in that] wherein the set of unique bit strings is stored in a first central memory [(38)], used combinations of identification codes and unique bit strings are stored in a second central memory [(40)], franking marks printed on documents are read in, combinations of identification codes and unique bit strings which are present in the read-in franking marks are stored in a third central memory [(42)] and are compared to the used combinations in the second central memory.--

--11. [A] The system for printing a franking mark [(28)] according to Claim 10, [characterised in that] wherein said system comprises a terminal [(2)] and a printing device [(20)], said terminal [(2)] being arranged to store, prior to step c, the unique bit string together with the identification

code, protected with the aid of a first message authentication code [and/]or protected by encoding, on an information carrier [(18)] with memory, and the printing device [(20)] is arranged to execute step c after reading the information carrier.--

--12. (amended) [A] The system according to Claim 11, [characterised in that] wherein the terminal is arranged to send a copy of either the unique bit string together with the identification code and the first message authentication code, or the unique bit string and the identification code in encoded form, to an exchange [(34)].--

--13. (twice amended) [A] The system according to Claim 11, [characterised in that] wherein the terminal [(2)] is arranged to store also, besides the unique bit string and the identification code, a terminal identification code, protected with the aid of the first message authentication code [and/]or protected by encoding, on the information carrier [(18)] with memory.--

--14. (twice amended) [A] The system according to Claim 11, [characterised in that] wherein the printing device [(20)] is arranged, after reading the information carrier [(18)], to render use of the unique bit string for printing a further franking mark on a further document impossible.--

--15. (twice amended) [A] The system according to Claim 11, [characterised in that] wherein the printing device [(20)] is arranged, after reading the information carrier [(18)], to check whether the value of a counter on the information carrier [(18)] lies within predefined limits, and, if this is the case, to execute step c and to adjust the value of the counter after reading, and, if this is not the case, to block step c.—

--16. (amended) [A] The system according to Claim 10, [characterised in that it comprises] further comprising a computer [(50)] and a printing device [(62)] connected thereto for executing step c.—

--17. (amended) [A] The system according to Claim 16, [characterised in that] wherein the system is provided with means [(70)] arranged remotely from the computer [(50)] to send the unique bit string, together with the identification code, protected with a first message authentication code [and/]or protected by encoding, to said computer [(50)] and to send a copy of said data to an exchange [(34)].—

--18. (amended) [A] The system according to Claim 16, [characterised in that] wherein the computer is provided with means [(64)] to print, with the aid of the printing device [(62)], the unique bit string together with the identification code, protected with a first message authentication code [and/]or protected by encoding, on the document, and optionally to send a copy of said data to an exchange [(34)].-

--19. (twice amended) [A] The system according to Claim 10, [characterised in that] wherein the identification code comprises a user identification code [and/]or printer identification code.--

--20. (twice amended) [A] The system according to Claim 10, [characterised in that] wherein the system is arranged to calculate and print, on the basis of the franking mark, a second message authentication code [and/]or to print the franking mark in encoded form.--

--21. (twice amended) [A] The system according to Claim 10, [characterised in that] wherein the system further comprises a second central memory [(40)] for storing combinations of identification codes and provided unique bit strings, central input means [(44)] for inputting franking marks printed on

documents, a third central memory [(42)] for storing the combinations of identification codes and unique bit strings present in the inputted franking marks, and processor means [(36)], connected to the central input means and the first, second, and third central memories, for mutually comparing the data in the second and third central memories.--

--22. (amended) [An exchange (34) provided with] A central station comprising:

a first central memory [(38)], with a set of unique bit strings,

a second central memory [(40)] for storing combinations of identification codes and provided unique bit strings, said combinations corresponding with franking marks [(28)] which are printed on a document [(22)],

central input means [(44)] for inputting franking marks printed on documents, [and]

a third central memory [(42) voor] for storing combinations of identification codes and unique bit strings present in the inputted franking marks, and

processor means [(36)], connected to the central input means and the first, second, and third central memories, for mutually comparing data in the second and third central memories.--

--23. (amended) [Means for a] A device [(20; 50) that is arranged] for printing a franking mark on a document [(22)], said device including means [at least being arranged] for receiving data from an information carrier [(18)], said data at least comprising a unique bit string originating from a set of unique bit strings, for compiling and making data available for the franking mark [(28)] for the document [(22)] in protected form, so that said device [(20; 50)] can print the franking mark [(28)] on the document securely, said franking mark at least comprising [the] said data as well as an identification code.

--24. (amended) [Means] The device according to Claim 23, [characterised in that they] wherein said means for receiving data are arranged to check, after reception of the data from the information carrier [(18)], whether the value of a counter on the information carrier [(18)] lies within predefined limits, and, if this is the case, to instruct the information carrier [(18)] to adjust the value of the counter, and, if this is not the case, to block the printing of the franking mark.--

IN THE ABSTRACT:

The Abstract of the Disclosure was amended as follows:

ABSTRACT OF THE DISCLOSURE

--A method and device[s] for printing a franking mark [(28)] on a document [(22) with the aid of the following steps: a] by making available a unique bit string; [b.] establishing an identification code; [c.] and securely printing the franking mark [(28)] on the document. [(22), said] The franking mark at least [comprising] includes information relating to the bit string and the identification code[; where the]. The bit string is selected from a centrally stored set of unique bit strings, and the unique bit strings which are made available for use are centrally registered.--